Dirigido a:
Eduardo Parraguez
khipu

FEBRERO
2020

INFORME TÉCNICO

Análisis de Tráfico de Datos febrero 2020

DOCUMENTO CONFIDENCIAL

https://nivel4.com

+56 2 2248 1368
Av Providencia 1208
Oficina 1204
Santiago, Chile.

1 Control de versiones

El siguiente cuadro muestra el historial de cambios sobre el presente documento.

Fecha	Autor	Versión	Comentarios
09-03-2019	Kevin Möller	1.0	Documentación

2 Introducción

La aplicación khipu permite a personas y empresas, pagar y cobrar, usando sus cuentas corrientes o cuentas vista del banco, de manera fácil y segura.

El terminal de pago de khipu es un navegador web especializado en pagos, por lo que, valida el correcto uso de las páginas de los bancos. Forma parte de un sistema que genera comprobantes de pago firmados electrónicamente, es reconocido por los principales antivirus del mundo y se instala desde fuentes oficiales de cada plataforma. khipu no almacena ni envía claves u contraseñas a sus servidores o a terceros.

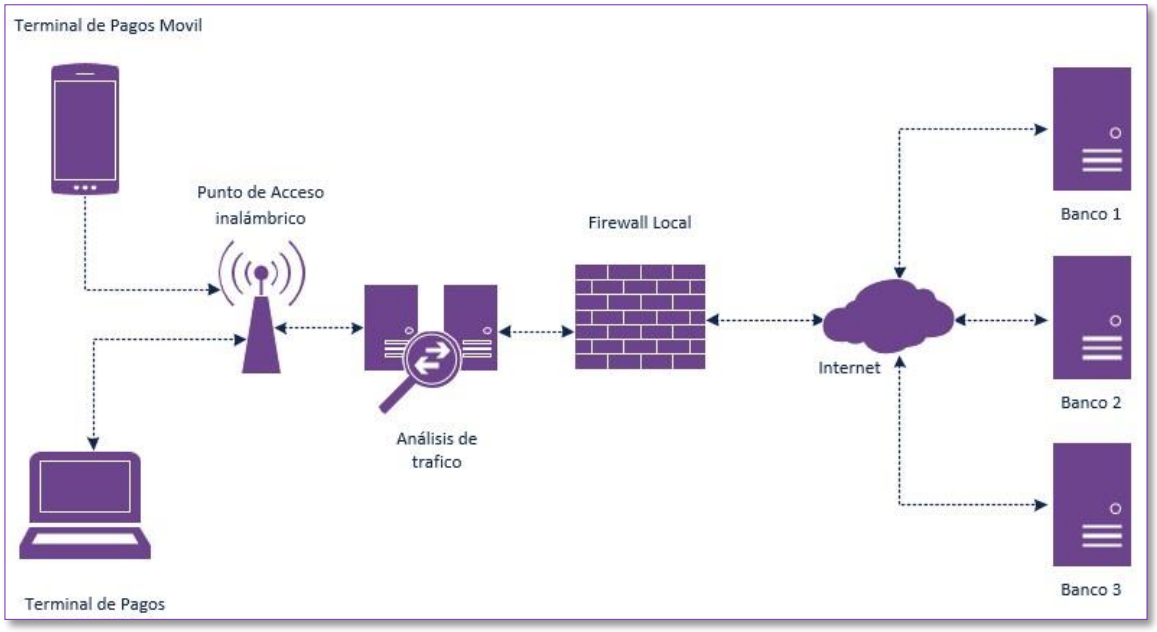
El presente análisis consiste en el monitoreo y análisis de todo el tráfico que genera la aplicación para las distintas plataformas, con el fin de detectar conexiones sospechosas. La revisión incluye la versión del terminal de pagos disponible para IOS y Android.

3 Objetivo

El análisis se realiza mensualmente, en un día y hora definida por Nivel4 sin que khipu conozca previamente esta información y tiene por objetivo certificar que la empresa no recibe las claves bancarias de sus usuarios ni las comparte con terceros. Adicionalmente, se realiza un Ethical Hacking al terminal de pago de iOS y Android.

4 Metodología

La metodología utilizada para la realización de este análisis de tráfico de red se basa en la utilización de un equipo que captura este tráfico entre el terminal de pagos y los bancos, de acuerdo con el siguiente diagrama:



Esta u otras metodologías pueden ser utilizadas por cualquier organización o persona natural que así lo requiera.

5 Ámbito

Para el actual período se registraron cambios para la aplicación de **iOS** en su HASH.

Plataforma	Versión	SHA256SUM
Android	7.4.4 - Ultima Actualización 20/01/2020	93fed81c119eb9d9acabbb649575fc80c0358ef0c85e12287553d3653209a970
iOS	7.16 - Ultima Actualización 21/01/2020	**27a58de60b8fe5da545520789538946be0712c12616840ce53b25cf525451841**

6 Análisis de tráfico de datos

Todo el tráfico analizado entre el terminal de pagos y los bancos se estableció mediante un **canal seguro** de comunicación. Si bien se detectó tráfico no seguro (HTTP) este corresponde a la validación del estado de los certificados SSL de algunos sitios, mediante OCSP y no durante la interacción con algún banco, en ningún caso se enviaron credenciales de usuario o datos de relacionados con las transacciones realizadas con el terminal de pagos al momento de realizar las pruebas. Finalmente, el resto del tráfico corresponde a consultas **DNS** y tráfico propio de una red local, como **NTP**, **NETBIOS**, **ARP**, entre otros.

En los siguientes puntos se detalla el tráfico detectado durante el uso de la aplicación evidenciando que las transacciones se realizan de forma segura y no se almacenan datos de usuario como, por ejemplo, claves del banco.

7 Análisis del terminal de pagos

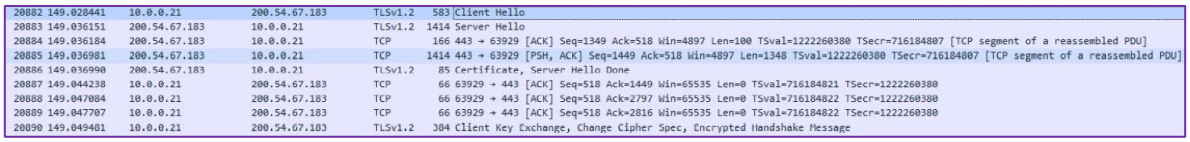
Como se puede ver en las siguientes tablas el tráfico que se genera al utilizar la aplicación de khipu solo se realiza con servidores confiables mediante canales seguros.

7.1 IPA

Origen	Destino	Tipo de Tráfico	Descripción
10.0.0.21	169.47.100.12 169.63.198.82 52.116.25.250	TLSv1.2	khipu
10.0.0.21	200.54.57.183	TLSv1.2	Banco ITAU
10.0.0.21	169.63.198.82	TLSv1.2	Banco Estado
10.0.0.21	104.16.206.140	TLSv1.2	Banco BICE

7.2 Tráfico TLS (seguro) entre el terminal de pagos y Banco “ITAU”

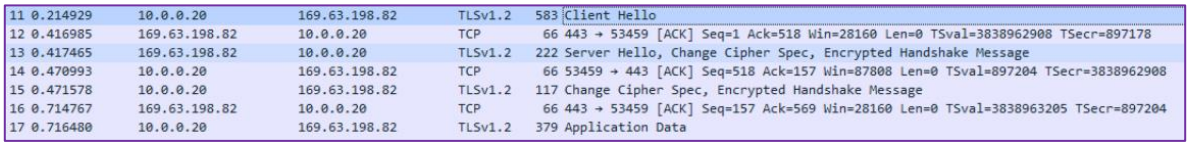
IPA



20882	149.028441	10.0.0.21	200.54.67.183	TLSv1.2	583 Client Hello
20883	149.036151	200.54.67.183	10.0.0.21	TLSv1.2	1414 Server Hello
20884	149.036184	200.54.67.183	10.0.0.21	TCP	166 443 → 63929 [ACK] Seq=1349 Ack=518 Win=4897 Len=100 TSval=1222260380 TSecr=716184807 [TCP segment of a reassembled PDU]
20885	149.036981	200.54.67.183	10.0.0.21	TCP	1414 443 → 63929 [PSH, ACK] Seq=1449 Ack=518 Win=4897 Len=1348 TSval=1222260380 TSecr=716184807 [TCP segment of a reassembled PDU]
20886	149.036990	200.54.67.183	10.0.0.21	TLSv1.2	85 Certificate, Server Hello Done
20887	149.044238	10.0.0.21	200.54.67.183	TCP	66 63929 → 443 [ACK] Seq=518 Ack=1449 Win=65535 Len=0 TSval=716184821 TSecr=1222260380
20888	149.047084	10.0.0.21	200.54.67.183	TCP	66 63929 → 443 [ACK] Seq=518 Ack=2797 Win=65535 Len=0 TSval=716184822 TSecr=1222260380
20889	149.047707	10.0.0.21	200.54.67.183	TCP	66 63929 → 443 [ACK] Seq=518 Ack=2816 Win=65535 Len=0 TSval=716184822 TSecr=1222260380
20890	149.049401	10.0.0.21	200.54.67.183	TLSv1.2	304 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

7.3 Tráfico TLS (seguro) entre el terminal de pagos y Banco “Estado”

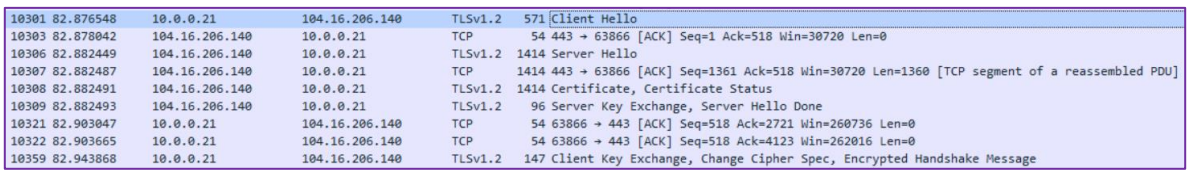
IPA



11	0.214929	10.0.0.20	169.63.198.82	TLSv1.2	583 Client Hello
12	0.416985	169.63.198.82	10.0.0.20	TCP	66 443 → 53459 [ACK] Seq=1 Ack=518 Win=28160 Len=0 TSval=3838962908 TSecr=897178
13	0.417465	169.63.198.82	10.0.0.20	TLSv1.2	222 Server Hello, Change Cipher Spec, Encrypted Handshake Message
14	0.470993	10.0.0.20	169.63.198.82	TCP	66 53459 → 443 [ACK] Seq=518 Ack=157 Win=87808 Len=0 TSval=897204 TSecr=3838962908
15	0.471578	10.0.0.20	169.63.198.82	TLSv1.2	117 Change Cipher Spec, Encrypted Handshake Message
16	0.714767	169.63.198.82	10.0.0.20	TCP	66 443 → 53459 [ACK] Seq=157 Ack=569 Win=28160 Len=0 TSval=3838963205 TSecr=897204
17	0.716480	10.0.0.20	169.63.198.82	TLSv1.2	379 Application Data

7.4 Tráfico TLS (seguro) entre el terminal de pagos y Banco “BCI”

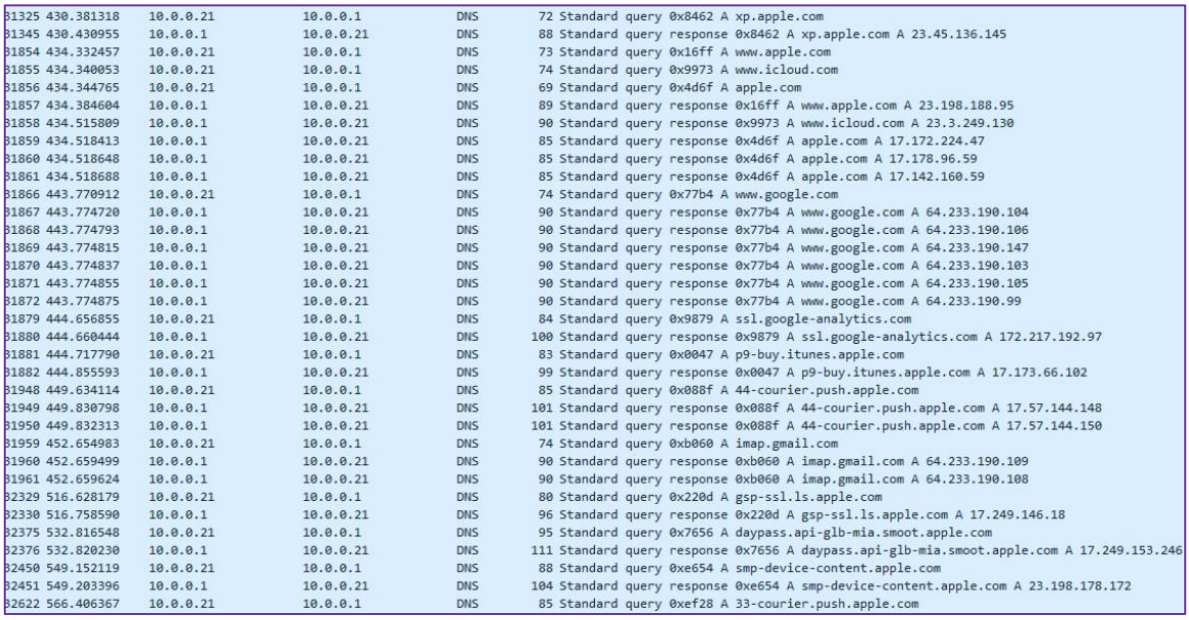
IPA



10301	82.876548	10.0.0.21	104.16.206.140	TLSv1.2	571 Client Hello
10303	82.878042	104.16.206.140	10.0.0.21	TCP	54 443 → 63866 [ACK] Seq=1 Ack=518 Win=30720 Len=0
10306	82.882449	104.16.206.140	10.0.0.21	TLSv1.2	1414 Server Hello
10307	82.882487	104.16.206.140	10.0.0.21	TCP	1414 443 → 63866 [ACK] Seq=1361 Ack=518 Win=30720 Len=1360 [TCP segment of a reassembled PDU]
10308	82.882491	104.16.206.140	10.0.0.21	TLSv1.2	1414 Certificate, Certificate Status
10309	82.882493	104.16.206.140	10.0.0.21	TLSv1.2	96 Server Key Exchange, Server Hello Done
10321	82.903047	10.0.0.21	104.16.206.140	TCP	54 63866 → 443 [ACK] Seq=518 Ack=2721 Win=260736 Len=0
10322	82.903665	10.0.0.21	104.16.206.140	TCP	54 63866 → 443 [ACK] Seq=518 Ack=4123 Win=262016 Len=0
10359	82.943868	10.0.0.21	104.16.206.140	TLSv1.2	147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

Tráfico DNS

IPA



```
31325 430.381318    10.0.0.21       10.0.0.1        DNS      72 Standard query 0x8462 A xp.apple.com
31345 430.430955    10.0.0.1        10.0.0.21       DNS      88 Standard query response 0x8462 A xp.apple.com A 23.45.136.145
31854 434.332457    10.0.0.21       10.0.0.1        DNS      73 Standard query 0x16ff A www.apple.com
31855 434.340053    10.0.0.21       10.0.0.1        DNS      74 Standard query 0x9973 A www.icloud.com
31856 434.344765    10.0.0.21       10.0.0.1        DNS      69 Standard query 0x4d6f A apple.com
31857 434.384604    10.0.0.1        10.0.0.21       DNS      89 Standard query response 0x16ff A www.apple.com A 23.198.188.95
31858 434.515809    10.0.0.1        10.0.0.21       DNS      90 Standard query response 0x9973 A www.icloud.com A 23.3.249.130
31859 434.518413    10.0.0.1        10.0.0.21       DNS      85 Standard query response 0x4d6f A apple.com A 17.172.224.47
31860 434.518648    10.0.0.1        10.0.0.21       DNS      85 Standard query response 0x4d6f A apple.com A 17.178.96.59
31861 434.518688    10.0.0.1        10.0.0.21       DNS      85 Standard query response 0x4d6f A apple.com A 17.142.160.59
31866 443.770912    10.0.0.21       10.0.0.1        DNS      74 Standard query 0x77b4 A www.google.com
31867 443.774720    10.0.0.1        10.0.0.21       DNS      90 Standard query response 0x77b4 A www.google.com A 64.233.190.104
31868 443.774793    10.0.0.1        10.0.0.21       DNS      90 Standard query response 0x77b4 A www.google.com A 64.233.190.106
31869 443.774815    10.0.0.1        10.0.0.21       DNS      90 Standard query response 0x77b4 A www.google.com A 64.233.190.147
31870 443.774837    10.0.0.1        10.0.0.21       DNS      90 Standard query response 0x77b4 A www.google.com A 64.233.190.103
31871 443.774855    10.0.0.1        10.0.0.21       DNS      90 Standard query response 0x77b4 A www.google.com A 64.233.190.105
31872 443.774875    10.0.0.1        10.0.0.21       DNS      90 Standard query response 0x77b4 A www.google.com A 64.233.190.99
31879 444.656855    10.0.0.21       10.0.0.1        DNS      84 Standard query 0x9879 A ssl.google-analytics.com
31880 444.660444    10.0.0.1        10.0.0.21       DNS     100 Standard query response 0x9879 A ssl.google-analytics.com A 172.217.192.97
31881 444.717790    10.0.0.21       10.0.0.1        DNS      83 Standard query 0x0047 A p9-buy.itunes.apple.com
31882 444.855593    10.0.0.1        10.0.0.21       DNS      99 Standard query response 0x0047 A p9-buy.itunes.apple.com A 17.173.66.102
31948 449.634114    10.0.0.21       10.0.0.1        DNS      85 Standard query 0x088f A 44-courier.push.apple.com
31949 449.830798    10.0.0.1        10.0.0.21       DNS     101 Standard query response 0x088f A 44-courier.push.apple.com A 17.57.144.148
31950 449.832313    10.0.0.1        10.0.0.21       DNS     101 Standard query response 0x088f A 44-courier.push.apple.com A 17.57.144.150
31959 452.654983    10.0.0.21       10.0.0.1        DNS      74 Standard query 0xb060 A imap.gmail.com
31960 452.659499    10.0.0.1        10.0.0.21       DNS      90 Standard query response 0xb060 A imap.gmail.com A 64.233.190.109
31961 452.659624    10.0.0.1        10.0.0.21       DNS      90 Standard query response 0xb060 A imap.gmail.com A 64.233.190.108
32329 516.628179    10.0.0.21       10.0.0.1        DNS      80 Standard query 0x220d A gsp-ssl.ls.apple.com
32330 516.758590    10.0.0.1        10.0.0.21       DNS      96 Standard query response 0x220d A gsp-ssl.ls.apple.com A 17.249.146.18
32375 532.816548    10.0.0.21       10.0.0.1        DNS      95 Standard query 0x7656 A daypass.api-glb-mia.smoot.apple.com
32376 532.820230    10.0.0.1        10.0.0.21       DNS     111 Standard query response 0x7656 A daypass.api-glb-mia.smoot.apple.com A 17.249.153.246
32450 549.152119    10.0.0.21       10.0.0.1        DNS      88 Standard query 0xe654 A smp-device-content.apple.com
32451 549.203396    10.0.0.1        10.0.0.21       DNS     104 Standard query response 0xe654 A smp-device-content.apple.com A 23.198.178.172
32622 566.406367    10.0.0.21       10.0.0.1        DNS      85 Standard query 0xef28 A 33-courier.push.apple.com
```

Tráfico HTTP

IPA

No se detectó tráfico HTTP durante el período Febrero.

Otro Tráfico

IPA

23284	156.694184	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42 10.0.0.21 is at 20:ee:28:db:b7:8d
24480	193.962479	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42 Who has 10.0.0.21? Tell 10.0.0.1
24481	194.073659	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42 10.0.0.21 is at 20:ee:28:db:b7:8d
30971	263.338461	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42 Who has 10.0.0.21? Tell 10.0.0.1
30972	263.395354	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42 10.0.0.21 is at 20:ee:28:db:b7:8d
31852	434.090435	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42 Who has 10.0.0.21? Tell 10.0.0.1
31853	434.094874	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42 10.0.0.21 is at 20:ee:28:db:b7:8d
32262	481.450453	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42 Who has 10.0.0.21? Tell 10.0.0.1
32263	481.508480	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42 10.0.0.21 is at 20:ee:28:db:b7:8d
32264	481.621690	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42 Who has 10.0.0.1? Tell 10.0.0.21
32265	481.621703	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42 10.0.0.1 is at bc:f6:85:21:26:0b
32373	521.898459	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42 Who has 10.0.0.21? Tell 10.0.0.1
32374	521.956672	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42 10.0.0.21 is at 20:ee:28:db:b7:8d
32453	549.290435	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42 Who has 10.0.0.21? Tell 10.0.0.1
32455	549.398889	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42 10.0.0.21 is at 20:ee:28:db:b7:8d
32720	572.586439	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42 Who has 10.0.0.21? Tell 10.0.0.1
32722	572.646644	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42 10.0.0.21 is at 20:ee:28:db:b7:8d
32733	601.002461	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42 Who has 10.0.0.21? Tell 10.0.0.1

8 Análisis SSL

El siguiente análisis tiene como objetivo determinar el nivel de seguridad en la implementación de SSL/TLS, se ejecutaron pruebas para determinar si se ve afectado por las vulnerabilidades conocidas hasta el momento

khipu.com – puerto 443

Vulnerabilidad	Identificador	Estado	Observaciones
Heartbleed	CVE-2014-0160	✓	No vulnerable
CCS	CVE-2014-0224	✓	No vulnerable
Ticketbleed	(CVE-2016-9244)	✓	No vulnerable
ROBOT	CVE-2017-17382	✓	No vulnerable
Secure Renegotiation	CVE-2009-3555	✓	No vulnerable
Secure Client-Initiated Renegotiation	CVE-2011-1473	✓	No vulnerable
CRIME	CVE-2012-4929	✓	No vulnerable
BREACH	CVE-2013-3587	✓	No vulnerable
POODLE	CVE-2014-3566	✓	No vulnerable

TLS_FALLBACK_SCSV	RFC 7507	✓	No vulnerable
SWEET32	CVE-2016-2183	✓	No vulnerable
FREAK	CVE-2015-0204	✓	No vulnerable
DROWN	CVE-2016-0703	✓	No vulnerable
LOGJAM	CVE-2015-4000	✓	No vulnerable
BEAST	CVE-2011-3389	✗	Potencialmente Vulnerable
LUCKY13	CVE-2013-0169	✓	No vulnerable
RC4	CVE-2013-2566 CVE-2015-2808	✓	No vulnerable

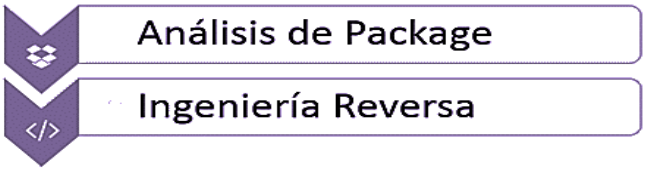
Se detectaron 1 potenciales vulnerabilidades en la implementación de SSL/TLS del sitio khipu.com las que afectan la confidencialidad de la información, sin embargo, esta vulnerabilidade tienen un alto grado de dificultad de explotación y se requieren condiciones especiales para su reproducción.

9 Referencias

Nombre	Link de referencia
Heartbleed	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
Ticketbleed	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9244
ROBOT	https://robotattack.org/
BREACH	http://breachattack.com/
POODLE	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555
FREAK	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0204
Logjam	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
BEAST	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3389
RC4	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2566
SLOTH	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7575
DROWN	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0800
Padding Oracle	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2107
SWEET32	https://cve.mitre.org/cgi-bin/cvenamcgi?name=CVE-2016-2183
LUCKY13	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0169

10 Ethical Hacking Mobile

Procesos automatizados y verificación manual



- Desempaquetado
- Decompilación
- Análisis de integridad
- Análisis de metadatos
- Análisis de strings
- Búsqueda con expresiones regulares
- Análisis en VirusTotal (malware)

Análisis de Package: Se analiza de forma estática el paquete compilado para los distintos sistemas operativos En el caso de iOS (para iPhone) el archivo IPA. Estos paquetes son sometidos a distintos tipos de análisis que verifican su integridad y seguridad.

Ingeniería Reversa: Durante este proceso las aplicaciones son descompiladas con el fin de realizar un análisis de código. Este tipo de análisis permite detectar malas prácticas de desarrollo, fugas de información mediante el código fuente, como direcciones IP, usuarios, claves. Además, permite conocer internamente los distintos componentes que utiliza la aplicación.

11 Análisis IPA

El resultado del análisis para la aplicación móvil es el siguiente:

Nombre	khipu7.13.ipa
SHA256	**27a58de60b8fe5da545520789538946be0712c12616840ce53b25cf525451841**
Tamaño	31 MB
Tipo	.ipa
URLs de interés	0
IPs encontradas	0
Emails encontrados	0

URLs detectadas

No se encontraron URLs en el análisis.

Direcciones de correo detectados

No se encontraron direcciones IP en el análisis.

Direcciones de correo detectados

No se encontraron direcciones.

12 Análisis de Malware

Se realizó un análisis utilizando distintos motores de antivirus, lo cual permite la detección de virus, gusanos, troyanos y todo tipo de malware que contengan el archivo *.apk (Android).

IPA	
Motor	**Estado**
Ad-Aware	✓
AegisLab	✓
AhnLab-V3	✓
Alibaba	✓
ALYac	✓
Antiy-AVL	✓
Arcabit	✓
Avast	✓
Avast-Mobile	✓
AVG	✓
Avira (no cloud)	✓

IPA	
AVware	✓
Babable	✓
Baidu	✓
BitDefender	✓
Bkav	✓
CAT-QuickHeal	✓
ClamAV	✓
CMC	✓
Comodo	✓
Cyren	✓
DrWeb	✓
Emsisoft	✓
ESET-NOD32	✓
F-Prot	✓
F-Secure	✓
Fortinet	✓

IPA	
GData	✓
Ikarus	✓
Jiangmin	✓
K7AntiVirus	✓
K7GW	✓
Kaspersky	✓
Kingsoft	✓
Malwarebytes	✓
MAX	✓
McAfee	✓
McAfee-GW- Edition	✓
Microsoft	✓
eScan	✓
NANO-Antivirus	✓
Panda	✓
Qihoo-360	✓

IPA	
Rising	✓
Sophos AV	✓
SUPERAntiSpywar e	✓
Symantec	✓
TACHYON	✓
Tencent	✓
TheHacker	✓
VBA32	✓
VIPRE	✓
ViRobot	✓
Yandex	✓
Zillya	✓
ZoneAlarm by Check Point	✓
Zoner	✓

13 Vulnerabilidades declaradas

A continuación, se listan las vulnerabilidades declaradas por terceros que pueden comprometer la seguridad de la aplicación y de khipu.com.

En este período de análisis se encontraron 1 potencial vulnerabilidad que afectan a la implementación de SSL/TLS, es **BEAST** (CVE-2011-3389). Esta vulnerabilidad afecta a la versión 1 de TLS. Si bien se encuentra mitigada al soportar la versión 1.1 y 1.2 de TLS, para corregirla correctamente, se debe desactivar el soporte para TLS 1.

Referencias

- https://www.openssl.org/blog/blog/2016/08/24/sweet32/
- http://www.isg.rhul.ac.uk/tls/
- https://raymii.org/s/tutorials/Strong_SSL_Security_On_nginx.html
- https://cipherli.st/

14 Anexos

#	Archivo	SHA256SUM
1	IOS20200310pcap	53a245d8f2d9f1d6561ce2b358da96ce9ed41e77ec76797ebaf04a6c85ad47e7